

Do Not Use the "%n" Format String Specifier

William L. Fithen, Software Engineering Institute [vita³]

Copyright © 2005 Carnegie Mellon University

2005-10-03

Careless use of "%n" format strings can introduce vulnerability.

Description

There are many kinds of vulnerability that can be caused by misusing format strings. Most of these are covered elsewhere, but this document covers one specific kind of format string vulnerability that is entirely unique for format strings. Documents in the public are inconsistent in coverage of these vulnerabilities.

In C, use of the "%n" format specification in `printf()` and `sprintf()` type functions can change memory values. Inappropriate design/implementation of these formats can lead to a vulnerability generated by changes in memory content. Many format vulnerabilities, particularly those with specifiers other than "%n", lead to traditional failures such as segmentation fault. The "%n" specifier has generated more damaging vulnerabilities. The "%n" vulnerabilities may have secondary impacts, since they can also be a significant consumer of computing and networking resources because large quantities of data may have to be transferred to generate the desired pointer value for the exploit.

Avoid using the "%n" format specifier. Use other means to accomplish your purpose.

References

- [Hoglund 04] Hoglund, Greg & McGraw, Gary. *Exploiting Software: How to Break Code*. Boston, MA: Addison-Wesley, 2004.
- [Newsham 00] Newsham, Tim. *Format String Attacks*.
<http://www.lava.net/~newsham/format-string-attacks.pdf>⁹ (2000).
- [scut 01] scut. *Exploiting Format String Vulnerabilities*.
<http://julianor.tripod.com/teso-fs1-1.pdf> (2001).
- [Seacord 05] Seacord, Robert C. *Secure Coding in C and C++*. Boston, MA: Addison-Wesley, 2005.

SEI Copyright

Carnegie Mellon University SEI-authored documents are sponsored by the U.S. Department of Defense under Contract FA8721-05-C-0003. Carnegie Mellon University retains copyrights in all material produced under this contract. The U.S. Government retains a non-exclusive, royalty-free license to publish or reproduce these documents, or allow others to do so, for U.S. Government purposes only

3. daisy:320 (Fithen, William L.)

9. <http://www.lava.net/%7Enewsham/format-string-attacks.pdf>

pursuant to the copyright license under the contract clause at 252.227-7013.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For inquiries regarding reproducing this document or preparing derivative works of this document for external and commercial use, including information about “Fair Use,” see the [Permissions](#)¹ page on the SEI web site. If you do not find the copyright information you need on this web site, please consult your legal counsel for advice.

Fields

Name	Value
Copyright Holder	SEI

Fields

Name	Value
is-content-area-overview	false
Content Areas	Knowledge/Guidelines
SDLC Relevance	Implementation
Workflow State	Publishable

1. <http://www.sei.cmu.edu/about/legal-permissions.html>